---

**Proceedings Paper:**
Foster, Simon David orcid.org/0000-0002-9889-9514, Gleirscher, Mario orcid.org/0000-0002-9445-6863 and Calinescu, Radu orcid.org/0000-0002-2678-9260 (Accepted: 2020) Towards Formal Verification of Control Algorithms for Autonomous Marine Vehicles. In: Proceeding of the 25th International Conference on Engineering of Complex Computer Systems (ICECCS 2020). IEEE (In Press)

---

# Towards Deductive Verification of Control Algorithms for Autonomous Marine Vehicles

Simon Foster[†], Mario Gleirscher[*†], Radu Calinescu[*†]
[†]*Department of Computer Science, University of York*, York, UK
[*]*Assuring Autonomy International Programme, University of York*, York, UK
simon.foster,mario.gleirscher,radu.calinescu@york.ac.uk

***Abstract*—The use of autonomous vehicles in real-world applications is often precluded by the difficulty of providing safety guarantees for their complex controllers. The simulation-based testing of these controllers cannot deliver sufficient safety guarantees, and the use of formal verification is very challenging due to the hybrid nature of the autonomous vehicles. Our work-in-progress paper introduces a formal verification approach that addresses this challenge by integrating the numerical computation of such a system (in GNU/Octave) with its hybrid system verification by means of a proof assistant (Isabelle). To show the effectiveness of our approach, we use it to verify differential invariants of an Autonomous Marine Vehicle with a controller switching between multiple modes.**

***Index Terms*—theorem proving, dynamical systems, autonomous vehicles, control systems, assurance cases**

## I. Introduction

Engineering controllers for autonomous vehicles requires a range of models, e.g. of the dynamics and of the control algorithms, for validating and verifying their key properties [1], [2]. Numerical computation (NC, e.g. with MATLAB) is a widely used simulation technique for model validation (i.e. closing the reality gap) and controller testing. However, simulation is, like testing, mostly limited to the demonstration of defects, since it can only consider a small fraction of the input space. For correctness, particularly to assess safety, full coverage of this space is desirable or mandatory. For hybrid systems, full coverage can be achieved only using symbolic reasoning techniques, such as deductive verification [3], due to the uncountable state space. We therefore need the translation of a validated model into a form amenable to verification in a proof environment such as Isabelle/HOL [4].

In this work, we investigate this translation for the case of a hybrid model of an Autonomous Marine Vehicle (AMV) and the formal verification of its safety properties. We describe the dynamics of the vehicle's motion, and controllers for waypoint approach and obstacle avoidance. We model the controller using hybrid state charts, including the mode switching for mitigating accidents between the operator and the safety controller. We simulate our model in the NC tool GNU/Octave,[1] for the purpose of validation against real-world trials, and translate this into an implementation of differential Dynamic Logic [3], [5] ($\mathsf{d}\mathcal{L}$) in Isabelle/HOL for deductive verification. To support this, we extend it to support matrices, discrete state, and a form of modular verification.

Our preliminary work serves as a template for how a translation from an NC tool to Isabelle can be achieved, and provides additional evidence that Isabelle provides a credible and flexible solution for hybrid systems verification. Our work is inspired by Mitsch et al. [6] who provide a generic verified model for collision avoidance in KeYmaera X [7]. We advance their work through provision of explicit support for transcendental functions in the system dynamics, a higher-level notation in our tool that bridges the semantic gap with control engineers, and access to Isabelle's automated proof facilities.

After an overview of the technologies we use in Section II, we present our approach to validation-based formal verification in Section III and close with a discussion in Section IV.

## II. Background

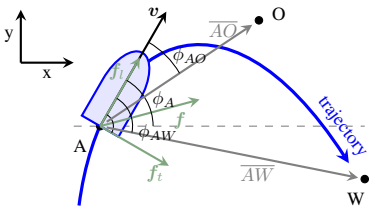
Isabelle/HOL [4] is a proof assistant for Higher Order Logic (HOL). It includes a functional specification language and an array of proof facilities, including *sledgehammer* [8], which integrates automated provers. Isabelle has a variety of mathematical libraries, notably for Multivariate Analysis [9] and Ordinary Differential Equations [10], [11] (ODEs), which provide the foundations for verification of hybrid systems.

Isabelle/UTP [12] is a semantic framework based on Hoare and He's Unifying Theories of Programming (UTP) [13], built on Isabelle/HOL. It supports diverse semantic models in a variety of paradigms, such as reactive, concurrent, and hybrid systems, and their application to verification. For example, it contains a tactic, *hoare-auto*, that automates verification of sequential programs using Hoare logic that uses *sledgehammer* to discharge verification conditions.

$\mathsf{d}\mathcal{L}$ is a logic for deductive verification of hybrid systems, which is supported by the KeYmaera X tool [7]. $\mathsf{d}\mathcal{L}$ can be used to prove invariants both of control algorithms and continuous dynamics, which makes it ideal for verifying hybrid systems. It avoids the need for explicit solutions to differential equations, by using a technique called *differential induction*. Recently, differential induction has been embedded into Isabelle [14] and Isabelle/UTP [5] to create differential Hoare logic ($\mathsf{d}\mathcal{H}$), which also supports verification of hybrid programs, but in a more general setting. In this paper, we apply $\mathsf{d}\mathcal{H}$ with Isabelle/UTP, and extend it.

[1] GNU/Octave. http://octave.sourceforge.io/

(a) AMV C-Worker 5




(b) AMV physics

Figure 1: An AMV in real and a model of its physics

## III. Approach

Our case study, the C-Worker 5[2] (Figure 1a) is an AMV designed to support hydrographic survey work. It operates in the open sea and so must avoid collisions with both static and dynamic obstacles, such as rocky outcrops and other vessels. We consider a safety controller that (1) avoids collisions with obstacles where possible by taking evasive maneuvers; and (2) mitigates the effects where avoidance is impossible. Our industrial partner, D-RisQ[3], is developing a safety controller called the Last Response Engine (LRE) [15] implementing the above functionality when the boat is operating autonomously. For verification, we focus on avoidance of static obstacles.

### A. Modelling the Dynamics and the Controller

*Modelling the AMV Dynamics:* The dynamical model should be close enough to reality to do NC and abstract enough to reduce the complexity of formal verification to a level appropriate for a credible assurance case [16], [17].

Indicated in Figure 1b, at time $t \in T$, we consider the velocity $\boldsymbol{v}_A = [v_A^x, v_A^y]^T$ and position $\boldsymbol{p}_A$ of the AMV, the position $\boldsymbol{p}_W$ of a next waypoint to be approached, and a set $\mathcal{O}$ of obstacles, the nearest described by its velocity $\boldsymbol{v}_O$ and position $\boldsymbol{p}_O$. $\boldsymbol{p}$ and $\boldsymbol{v}$ are vectors in planar coordinates $(x, y)$ over $\mathbb{R}^2$. These parameters form a state space $\mathcal{X}$ with tuples

$$\boldsymbol{x} = [\boldsymbol{p}_A, \boldsymbol{v}_A, \boldsymbol{p}_O, \boldsymbol{v}_O]^T.$$

Below, we abbreviate $\boldsymbol{p}_E$ by $E$ where $E \in \{A, O, W\}$. We also consider parameters calculated from $\boldsymbol{x}$, such as the distance to the next waypoint $\left\|\overline{AW}\right\|$ or the angle $\phi_{AO}$ between the AMV velocity vector and the distance vector $\overline{AO}$.

For sake of simplicity, we consider the AMV as a particle with mass $m$ and formulate its dynamics as the following system of ordinary differential equations

$$\dot{\boldsymbol{p}}_A = \boldsymbol{v}, \quad \dot{\boldsymbol{v}}_A = \boldsymbol{f}/m, \quad \dot{\boldsymbol{v}}_O = \boldsymbol{0}, \quad \text{and} \quad \dot{\boldsymbol{p}}_O = \boldsymbol{0} \qquad (1)$$

where $\boldsymbol{f}/m$ implements Newton's second law of the kinetics of particle masses relating a force applied to the vehicle and this vehicle's acceleration at time $t$. To remain in scope of our investigation, we further simplify the AMV dynamics, omitting disturbances (e.g. crosswind) and perturbations (e.g. flow resistance), and restricting our analysis to static obstacles.

[2]C-Worker 5. https://www.asvglobal.com/product/c-worker-5/
[3]D-RisQ Software Systems. http://www.drisq.com/

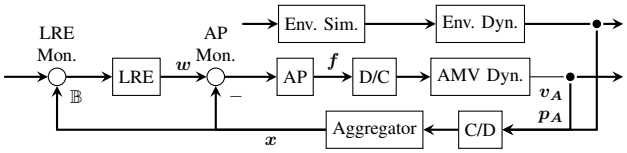



Figure 2: Block structure diagram of the dynamical model and the two-layered controller with the corresponding monitors

*Modelling the AMV Controller:* Figure 2 shows the structure of the plant consisting of the dynamical model of the AMV and its environment (as explained before) and a two-layered controller comprising the autopilot (AP) and the LRE.

The *discrete low-level control* of the vehicle is facilitated by the AP through generating the propulsive force $\boldsymbol{f}$ of the AMV as an input to the AMV dynamics. Within the frame of reference of the trajectory of the AMV, we model the AMV's single thruster by calculating two components of $\boldsymbol{f}$, the longitudinal (or tangential) acceleration force $\boldsymbol{f}_l$ collinear with the AMV's velocity $\boldsymbol{v}$ and the radial acceleration force $\boldsymbol{f}_t$ perpendicular to $\boldsymbol{f}_l$, such that

$$\boldsymbol{f} = \boldsymbol{f}_l + \boldsymbol{f}_t = f_l \begin{bmatrix} \cos(\phi_A) \\ \sin(\phi_A) \end{bmatrix} + f_t \begin{bmatrix} -\mathrm{sgn}(\phi_A)\sin(\phi_A) \\ \mathrm{sgn}(\phi_A)\cos(\phi_A) \end{bmatrix}.$$

The *discrete high-level control* of the AMV is partially facilitated by the LRE through switching between several operating modes: an Operator Control Mode (OCM), a Main Operating Mode (MOM), a High Caution Mode (HCM), and a Collision Avoidance Mode (CAM). When in OCM, the operator has responsibility for the AMV. When in MOM, the AMV navigates towards the next waypoint at maximum speed. If it gets close to, but not on collision course with, an obstacle then it switches to HCM. If a potential future collision is detected, it transitions to CAM to make evasive maneuvers. Each of these modes provides the AP with a particular setpoint $\boldsymbol{w} = [rs, \boldsymbol{p}_W]^T$ (i.e. target speed and location of next waypoint) for the calculation of $\boldsymbol{f}$ by the AP as described by the hybrid automaton in Figure 3

$$f_l = k_p^l \cdot |rs - \|\boldsymbol{v}_A\|\,| \qquad (2)$$

$$f_t = \begin{cases} k_p^t \cdot \phi_{AW}, & \text{in MOM} \\ k_p^t \cdot \mathrm{sgn}(\phi_{AW}) \cdot f_{max}, & \text{in CAM/HCM} \end{cases} \qquad (3)$$

In this example, we use a simple proportional controller for $\boldsymbol{f}$ with directional proportionality factors $k_p$ as shown in Equation (2). For obstacle avoidance manoeuvres, we calculate the *safe braking distance* by

$$d_{sb} = \frac{sb \cdot \|\boldsymbol{v}_A\|^2 \cdot m}{-2 \cdot k_p^b \cdot f_{max}} \qquad (4)$$

with a safety margin $sb$ to capture modelling uncertainty and define the *near-Obstacle (nO)* and *on-Collision-Course (oCC)* hazards as the predicates

$$nO \equiv \left\|\overline{AO}\right\| < d_{sb} \quad \text{and} \quad oCC \equiv nO \wedge |\phi_{AO}| < \epsilon_\phi. \qquad (5)$$

In MOM, we add a *hysteresis* $\epsilon_h$ to $\epsilon_\phi$ in order to delay manoeuvre cancellation. Figure 3 describes the overall behaviour

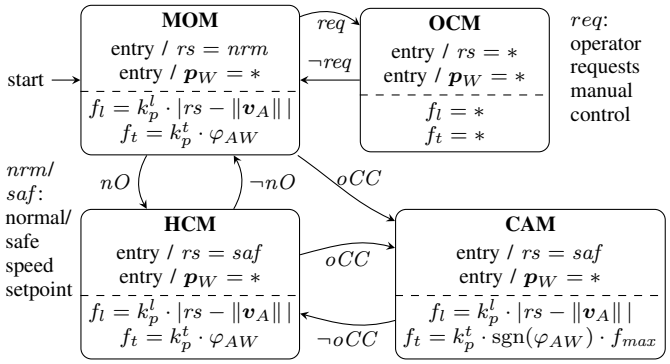



Figure 3: Behaviour of the LRE and AP as a Moore machine, the $*$-operator indicates a non-deterministic assignment

of the LRE switching between the four modes to provide $\boldsymbol{w}$ to the AP. From the components LRE and AP shown in Figure 2 and from the modes in Figure 3, one can then derive interfaces for the detailed software design.

*Note on Abstraction:* The transition from the discrete LRE and AP to the continuous AMV physics is accomplished by a conversion of (D)iscretely timed $\boldsymbol{f}$ inputs in form of (C)ontinuous, piece-wise constant signals, processed by actuators. Vice versa, the digital controller (particularly, the Aggregator in Figure 2) samples the environment through sensors at a certain rate. Figure 2 indicates this abstraction by D/C and C/D converters. Although we chose to apply this abstraction to the generation of $\boldsymbol{f}$, in practice, this will happen inside the thrusters where, e.g. digital signals control a servo motor of a combustion engine and a rudder to generate $\boldsymbol{f}$.

*Simulation:* We implemented the AMV model in an integrator-based simulator in GNU/Octave. We derived parameters, such as weight, maximum speed and propulsive force, from the C-Worker 5 specification. We identified controller constants, such as $k_p^l$, during simulation. Figure 4 shows a trajectory of the AMV (green dot) turning to make its way to the next waypoint $W$ (blue dot) while circumventing a floating obstacle (pink dot). The initial state $\boldsymbol{x}_0 \in \mathcal{X}$ is set to

$$\boldsymbol{x}_0 = [\underbrace{-.5, -3.8}_{\boldsymbol{v}_A\,[m/s]}, \underbrace{-10, -10}_{\boldsymbol{p}_A\,[m]}, \underbrace{0, 0}_{\boldsymbol{v}_{O_1}\,[m/s]}, \underbrace{-12, -18}_{\boldsymbol{p}_{O_1}\,[m]}, \dots]^T$$

and the simulation run for the constants $rs = 4m/s$, $\boldsymbol{p}_W = [0, 0]^T$, and the time interval $T = [0, 35]$ sec. Note, the 2D trajectory from the AMV exhibits a deviation from its course where $oCC$ turned true. The lower middle graph shows this as the event of $d_{sb} \approx 13 > |\overline{AO}|$ where the magenta curve touches the red curve at $t \approx 5s$, simultaneous to the reduction of $\|\boldsymbol{v}_A\|$ after the switch to $CAM$ (cf. top right graph).

*Beyond Simulation:* Our quest for covering the input space (Section I) requires us to ask how we can know that from wherever in $\mathcal{X}$ we start, wherever an obstacle is, in whatever interval $T$ we evaluate a trajectory, will the AMV always steer away from an obstacle in CAM, will it always reduce speed in HCM, will it reach the next waypoint within a given time in MOM? Such questions require a more fundamental investigation of the model discussed in the next section.

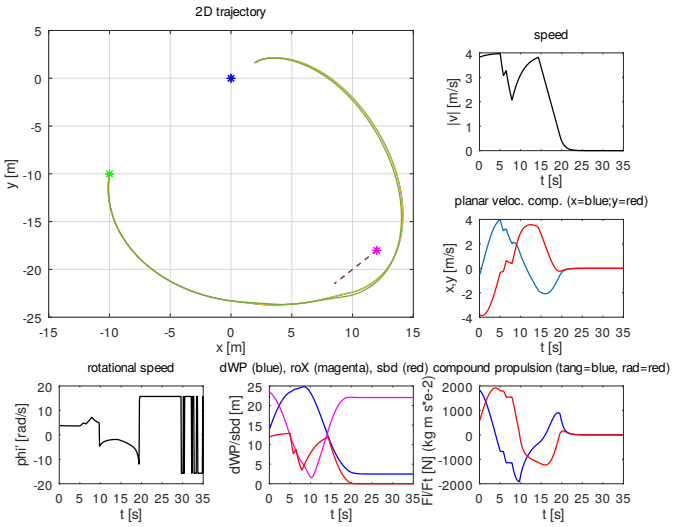



Figure 4: Simulation: the AMV (green dot) approaching next waypoint (blue dot) while crossing an obstacle (pink dot)

## B. Verification

Here, we use Isabelle/dH [5] to support deductive verification of the AMV. We extend it with matrices, discrete variables, and modular reasoning [12]. Along with standard Hoare logic laws, Isabelle/dH includes the key dL rules as theorems, including differential induction and cut[4].

**Theorem III.1.** *Differential Induction and Cut*

$$\frac{\mathit{differentiable}(P) \wedge (B \Rightarrow \mathcal{L}_F(P))}{\{P\}\,\langle \dot{\boldsymbol{x}} = F(\boldsymbol{x}) \mid B(\boldsymbol{x})\rangle\,\{P\}} \tag{6}$$

$$\frac{\{P\}\,\langle F \mid B\rangle\,\{P\} \quad \{Q\}\,\langle F \mid B \wedge P\rangle\,\{Q\}}{\{P \wedge Q\}\,\langle F \mid B\rangle\,\{Q\}} \tag{7}$$

Here, $\langle \dot{\boldsymbol{x}} = F(\boldsymbol{x}) \mid B(\boldsymbol{x})\rangle$ is a system of ODEs with an evolution domain $B$. The dynamical system is permitted to evolve provided that the ODEs in $F$, and predicate $B$, are satisfied for all points on the solution trajectory. (6) states that if $P$ is everywhere differentiable, and its differentiated form follows from $B$, then $P$ is an invariant. (7) shows that if we can prove that $P$ is invariant, then we can use it as an axiom of the dynamics to prove that $Q$ is also an invariant [3].

We extend [5] with automated Lie derivative [18] evaluation. ODEs are encoded as a vector field $F : \mathbb{R}^n \to \mathbb{R}^n$. $\mathcal{L}_F(P)$ denotes the Lie derivative of the predicate $P$ along $F$. $P$ is restricted to the form $e\ R\ f$, for $R \in \{=, \leq, <\}$, over differentiable expressions $e, f : \mathbb{R}^n \to \mathbb{R}$, and their conjunctions and disjunctions, such as $2x \leq 5$. We exemplify $\mathcal{L}$ below.

$$\mathcal{L}_F(e \leq f) = (\mathcal{L}_F(e) \leq \mathcal{L}_F(f)) \tag{8}$$

$$\mathcal{L}_F(e + f) = \mathcal{L}_F(e) + \mathcal{L}_F(f) \tag{9}$$

$$\mathcal{L}_F(e \cdot f) = \mathcal{L}_F(e) \cdot f + e \cdot \mathcal{L}_F(f) \tag{10}$$

$$\mathcal{L}_F(\sin(e)) = \mathcal{L}_F(e) \cdot \cos(e) \tag{11}$$

$$\mathcal{L}_F(x) = (\lambda s : \mathbb{R}^n .\, \mathit{get}_x\ F(s)) \tag{12}$$

[4]Proofs can be found in our repository (https://github.com/isabelle-utp/utp-main) and the accompanying links.

These are largely standard, such as the product rule (10). Of note, (12) shows the treatment of a continuous variable $x : \mathbb{R}$. We encode mutable variables using lenses [19], which are pairs

$$(x : V \Longrightarrow S) \triangleq (\mathit{get}_x : S \to V, \mathit{put}_x : S \to V \to S)$$

for some suitable state space $S$ and variable type $V$, that obey intuitive algebraic laws [12]. Here, we require that every continuous variable has a bounded linear *get* function, which is satisfied, for example, when $x$ is a projection of a Euclidean space. The derivative of $x$ is an expression that applies the *get* function to the derivative of the state ($F(s)$). This can be seen as a semantic substitution of $x$ by its derivative [12].

Invariants can contain transcendental functions such as sin and $log$. We also support equalities between arbitrary Euclidean spaces, such as matrices. To close the gap between Octave and Isabelle, we have implemented a smart matrix parser. A matrix in Isabelle is represented by a function: $A\ mat[M, N] \triangleq N \to M \to A$, where $N$ and $M$ are finite types denoting the dimensions, and $A$ is the element type, usually $\mathbb{R}$. Thus, the Isabelle type system can be used to ensure that matrix expressions are well-formed. We use the syntax

$$\left[[x_1^1, x_2^1, \cdots x_n^1], \cdots, [x_1^m, x_2^m, \cdots, x_n^m]\right]$$

to represent a $m$ by $n$ matrix in Isabelle, which is a list of lists. Our parser can infer the dimensions of a well-formed matrix, and produce suitable dimension types, which aids proof. Moreover, we have proved theorems that allow symbolic evaluation of certain vector operations, for example:

$$[x_1, y_1] + [x_2, y_2] = [x_1 + x_2, y_1 + y_2]$$
$$n \cdot [x, y] = [n \cdot x, n \cdot y]$$

We also define the matrix lens

$$\mathit{mat\text{-}lens}(m : M, n : N) : A \Longrightarrow A\ mat[M, N]$$

which accesses an element. With it, we can model both variables that refer to an entire matrix and also its elements.

We have developed a tactic in Isabelle/dℋ called *dInduct*, which automates the application of Theorem III.1 by determining whether $P$ is indeed differentiable everywhere, and if so applying differentiation and substitution. The resulting predicate can be discharged, or refuted, using Isabelle's tactics.

Hybrid systems in Isabelle/dℋ follow the pattern of $Sys \triangleq (Ctrl\ ;\ Dyn)^\star$, where the controller and dynamics iteratively take turns in updating the variables [6]. Proving a safety property $P$ of $Sys$ entails finding an invariant $I$ both of $Ctrl$ and $Dyn$, such that $I \Rightarrow P$. Isabelle/dℋ splits the state space of a hybrid system into its continuous and discrete variables. Continuous variables change during evolution, but discrete variables are constant and updated only by assignments.

The continuous state space ($\Sigma_C$) must form a Euclidean space, and so is typically composed of reals, vectors, and matrices. There are no restrictions on the discrete state space, and it may use any Isabelle data type.

*Case Study:* We describe each of the continuous variables using lenses, e.g. $\boldsymbol{p}, \boldsymbol{v} : \mathbb{R}\ mat[1, 2] \Longrightarrow \Sigma_C$[5]. In addition to those mentioned in §III-A, we also include $\boldsymbol{a} : \mathbb{R}\ mat[1, 2]$ for the acceleration, and $s : \mathbb{R}$, for the linear speed. Technically, $s$ can be derived as $\|v\|$, but its inclusion makes proving invariants easier. Most are monitored variables of the environment, except $\boldsymbol{a}$, which is updated by the AP. The discrete variables include waypoint location ($\boldsymbol{wp} : \mathbb{R}^2$); obstacle set ($ob : \mathbb{P}(\mathbb{R}^2)$); linear speed and heading set points ($rs, rh : \mathbb{R}$); force vector ($\boldsymbol{f} : \mathbb{R}^2$); and mode ($m : \{\mathit{OCM}, \mathit{MOM}, \mathit{HCM}, \mathit{CAM}\}$). Next, we describe the dynamics.

**Definition III.2** (AMV Dynamics)**.**

$$dyn_{AV} \triangleq \begin{pmatrix} \dot{t} = 1;\ \dot{\boldsymbol{p}} = \boldsymbol{v};\ \dot{\boldsymbol{v}} = \boldsymbol{a};\ \dot{\boldsymbol{a}} = 0; \\ \dot{s} = \dfrac{\boldsymbol{v} \cdot \boldsymbol{a}}{s} \lhd s \neq 0 \rhd \|\boldsymbol{a}\|\,; \\ \dot{\phi} = acos\left(\dfrac{(\boldsymbol{v} + \boldsymbol{a}) \cdot \boldsymbol{v}}{\|\boldsymbol{v} + \boldsymbol{a}\| \cdot \|\boldsymbol{v}\|}\right) \lhd s \neq 0 \rhd 0 \end{pmatrix}$$

$$ax_{AV} \triangleq \left( 0 \leq s \wedge s \leq S \wedge s \cdot \begin{bmatrix} \sin(\phi) \\ \cos(\phi) \end{bmatrix} = \boldsymbol{v} \wedge t < \epsilon \right)$$

$$Dyn \triangleq t := 0\ ;\ \langle dyn_{AV} \mid ax_{AV} \rangle$$

Dynamics $dyn_{AV}$ is a system of six ODEs. For the linear speed derivative, we consider the special case when $s = 0$, where the speed derivative is derived from $\boldsymbol{a}$, and the rotational speed is 0. We also axiomatise some properties of the dynamics in $ax_{AV}$: (1) the linear speed must be in $[0, S]$; (2) $\boldsymbol{v}$ must be the same as $s$ multiplied by the orientation unit vector; (3) time must not advance beyond $\epsilon$, which puts an upper bound on the time between control decisions.

Next, we model the LRE, which is encoded as a set of guarded commands derived from Figure 3. In each iteration, the LRE updates state variables and can transition to a different state. Whilst in MOM, the speed set point is the maximum speed (S), and the LRE invokes the command *steerToWP* that updates the heading towards the current way point.

**Definition III.3** (Simplified LRE)**.** $LRE \triangleq$

$$\begin{pmatrix} m = \mathit{MOM} \to \begin{pmatrix} rs := S\ ;\ \mathit{steerToWP}\ ; \\ \textbf{if}\ \mathit{oCC}\ \textbf{then}\ m := \mathit{CAM}\ \textbf{fi}\ ; \\ \textbf{if}\ \exists \boldsymbol{o} \in ob.\ \|\boldsymbol{o} - \boldsymbol{p}\| \leq D \\ \textbf{then}\ m := \mathit{HCM}\ ;\ rs := H\ \textbf{fi} \end{pmatrix} \\ m = \mathit{HCM} \to \begin{pmatrix} rs := H\ ;\ \mathit{steerToWP}\ ; \\ \textbf{if}\ \forall \boldsymbol{o} \in ob.\ \|\boldsymbol{o} - \boldsymbol{p}\| > D \\ \textbf{then}\ m := \mathit{MOM}\ \textbf{fi} \end{pmatrix} \\ m = \mathit{OCM} \to \textbf{skip} \\ m = \mathit{CAM} \to \cdots \end{pmatrix}$$

If oCC is detected the LRE transitions to CAM. If nO holds but not oCC, then the LRE switches to HCM. From HCM, the speed set point is decreased to $H$. Once the AMV is no longer close to an obstacle, the LRE may return to MOM. OCM exhibits no behaviour since the operator provides the control inputs. Finally, CAM is where collision avoidance procedures are executed. Its behaviour is left unspecified for now. The final component we model is the autopilot.

[5]We omit the $A$ subscripts for brevity.

```
abbreviation "AP ≡
  if ‖rs - &c:s‖ > sε
    then ft := sgn(rs - &c:s)*min(kpgv * ‖rs - &c:s‖) fmax
    else ft := 0 fi ;;
  if ‖rh - &c:φ‖ > φε
    then fl := sgn(rh - &c:φ)*min(kpgr * ‖rh - &c:φ‖) fmax
    else fl := 0 fi ;;
  F := fl *R [[cos(&c:φ), sin(&c:φ)]]
     + ft *R [[sin(&c:φ), cos(&c:φ)]] ;;
  c:a := F /R m"
```

Figure 5: Autopilot in Isabelle/UTP

**Definition III.4** (Autopilot Controller). $AP \triangleq$

**if** $\|rs - s\| > s_\epsilon$
**then** $ft := \mathrm{sgn}(rs - s) \cdot \min\left(\begin{array}{c} kp_{gv} \cdot \|rs - s\|, \\ f_{max} \end{array}\right)$
**else** $ft := 0$ **fi** ;
**if** $\|rh - \phi\| > \phi_\epsilon$
**then** $fl := \mathrm{sgn}(rh - \phi) \cdot \min\left(\begin{array}{c} kp_{gr} \cdot \|rh - \phi\|, \\ f_{max} \end{array}\right)$
**else** $fl := 0$ **fi** ;
$\boldsymbol{f} := fl \cdot \begin{bmatrix} \cos(\phi) \\ \sin(\phi) \end{bmatrix} + ft \cdot \begin{bmatrix} \sin(\phi) \\ \cos(\phi) \end{bmatrix}$ ; $\boldsymbol{a} := \boldsymbol{f}/m$

The AP takes $rs$ and $rh$ as inputs, computes $\boldsymbol{f}$, and calculates $\boldsymbol{a}$. The constants $s_\epsilon$ and $\phi_\epsilon$ limit the controller activity when the speed is close to the set point. Its representation in Isabelle/UTP is shown in Figure 5. Continuous variables are distinguished using the namespace **c**, e.g. **c**:$x$. Scalar multiplication and division are distinguished operators, $n *_R \boldsymbol{x}$ and $\boldsymbol{x} /_R n$. Finally, we describe the overall AMV behaviour.

**Definition III.5.** $AMV \triangleq (LRE \,;\, AP \,;\, Dyn)^\star$

The LRE executes first to determine the new speed set points. Following this, the autopilot calculates the new acceleration vector. Finally, the dynamical system evolves the continuous variables for up to $\epsilon$ seconds, and then the cycle begins again. We will now proceed to verify some properties of the system using Isabelle/dH. We begin with some structural properties.

**Theorem III.6** (Structural Properties).

- $LRE$ ***nmods*** $\{t, \boldsymbol{p}, \boldsymbol{v}, \boldsymbol{a}, s, \phi\}$
- $AP$ ***nmods*** $\{t, \boldsymbol{p}, \boldsymbol{v}, s, \phi\}$
- $Dyn$ ***nmods*** $\{\boldsymbol{wp}, ob, rs, rh, ft, fl, \boldsymbol{f}, m\}$

$P$ ***nmods*** $A$ means that $P$ does not modify the variables in $A$. It enables modular verification using the following theorem:

$$S \textbf{ nmods } \boldsymbol{x} \implies \{p(\boldsymbol{x})\}\, S\, \{p(\boldsymbol{x})\}$$

If $\boldsymbol{x}$ is not modified by $S$, then any predicate in $\boldsymbol{x}$ is invariant. We can verify that the LRE does not modify any of the continuous variables, as it only updates the (discrete) set points. The AP modifies only the continuous variable $\boldsymbol{a}$. We can prove that $ax_{AV}$ is an invariant of both $LRE$ and $AP$, and therefore of the entire system. The dynamics can potentially change any of the continuous variables, but does not change any of the discrete variables. These structural properties are automatically proved, and are useful to ensure structural well-formedness of a controller under development.

```
lemma no_turn_when_straight:
 "{&c:a • &c:v = ‖&c:a‖ * ‖&c:v‖ ∧ &c:φ = «X»}
   ODE
  {&c:φ = «X»}"
  apply (rule dCut_split', fact collinear_vector_accel)
  apply (dInduct_auto)
  apply (smt norm_ge_zero)+
  done
```

Figure 6: Example proof in Isabelle/dH

We next prove some invariants of the system using dH.

**Theorem III.7** (Collinearity of $\boldsymbol{v}$ and $\boldsymbol{a}$).

$$\{\boldsymbol{a} \cdot \boldsymbol{v} = \|\boldsymbol{a}\| \cdot \|\boldsymbol{v}\|\}\, Dyn\, \{\boldsymbol{a} \cdot \boldsymbol{v} = \|\boldsymbol{a}\| \cdot \|\boldsymbol{v}\|\}$$

*Proof.* We first prove that $\boldsymbol{a} \cdot \boldsymbol{v} \geq 0$ and $(\boldsymbol{a} \cdot \boldsymbol{v})^2 = (\boldsymbol{a} \cdot \boldsymbol{a}) \cdot (\boldsymbol{v} \cdot \boldsymbol{v})$ are both invariants by theorem III.1. We can then show these are equivalent with $\boldsymbol{a} \cdot \boldsymbol{v} = \|\boldsymbol{a}\| \cdot \|\boldsymbol{v}\|$. □

Collinearity means that $\boldsymbol{v}$ and $\boldsymbol{a}$ have the same direction and the AMV is travelling straight. A corollary is below.

$$\left\{\boldsymbol{a} \cdot \boldsymbol{v} = \|\boldsymbol{a}\| \cdot \|\boldsymbol{v}\|\right\} Dyn \left\{\boldsymbol{p} = \frac{t^2}{2} \cdot \boldsymbol{a} + t \cdot old(\boldsymbol{v}) + old(\boldsymbol{p})\right\}$$

This states that if the AMV is travelling in a straight line, then its position can be obtained through integration of $\dot{\boldsymbol{p}}$. By Theorem III.6, collinearity is also trivially an invariant of the $LRE$, since it does not modify any continuous variables.

We show proof of a further corollary in Figure 6 in Isabelle/UTP: if the AMV is moving straight, then the heading is constant. We introduce a ghost variable $X$ for the current heading $\phi$. The proof proceeds by performing a differential cut (*dCut_split'*), which allows us to assume collinearity in the dynamical system. Theorem III.7 corresponds to the fact *collinear_vector_accel* in Isabelle. Then, we use differential induction via the *dInduct_auto* tactic, which also applies algebraic simplification laws. Finally, we call *sledgehammer* which provides SMT proofs to discharge the remaining proof obligation, which is essentially $\boldsymbol{a} \cdot \boldsymbol{v} = \|\boldsymbol{a}\| \cdot \|\boldsymbol{v}\| \Rightarrow \dot{\phi} = 0$. This technique allows us to harness all the mathematical results proved in HOL and HOL-Analysis in our proofs [9], [10].

Collinearity is established by $AP$ when the heading set point is the same as the actual heading:

**Theorem III.8** (Autopilot Collinearity).

$$\left\{\begin{array}{c} \|rh - \phi\| < \phi_\epsilon \wedge 0 \leq s \wedge \\ s \leq rs \wedge \boldsymbol{v} = s \cdot \begin{bmatrix} \sin(\phi) \\ \cos(\phi) \end{bmatrix} \end{array}\right\} AP \left\{\begin{array}{c} \boldsymbol{a} \cdot \boldsymbol{v} \\ = \|\boldsymbol{a}\| \cdot \|\boldsymbol{v}\| \end{array}\right\}$$

*Proof.* Hoare logic reasoning and vector arithmetic. A crucial fact is that $[\sin(\phi), \cos(\phi)] \cdot [\sin(\phi), \cos(\phi)] = 1$. □

The theorem shows that if the linear speed is between 0 and $rs$, $\phi$ and $rh$ are sufficiently close, and $\boldsymbol{v}$ can be derived from the linear speed and heading, then afterwards $\boldsymbol{a}$ and $\boldsymbol{v}$ are again collinear. Now, by the sequential composition law, we can compose this with III.7 to obtain the same Hoare triple for $AP \,;\, Dyn$. Finally, we show a property of the LRE.

$$\left\{\begin{array}{c} m = MOM \wedge \\ \|ang(\boldsymbol{wp} - \boldsymbol{p}) - \phi\| \leq \phi_\epsilon \\ \wedge\, (\exists \boldsymbol{o} \in ob.\, \|\boldsymbol{p} - \boldsymbol{o}\| \leq D) \end{array}\right\} LRE \left\{\begin{array}{c} m = HCM \\ \wedge\, rs = H \wedge \\ \|rh - \phi\| \leq \phi_\epsilon \end{array}\right\}$$

This shows that if the LRE is in MOM, and the heading is currently towards the waypoint, but an obstacle is close, then it will transition to HCM, drop the set point speed to $H$ and the requested heading remains close to the actual heading.

## IV. Discussion and Conclusion

In this paper, we have made preliminary steps to integrating NC with theorem proving in Isabelle. Octave and Isabelle's approaches to mathematics are, in many ways, quite different. Octave is focused on efficient NC, whereas Isabelle is based on foundational mathematics and proof. Nevertheless, our investigation indicates that they can effectively be used together.

Most of the required Octave functions, such as, sin, sgn, and the vector operations are present in Isabelle, and are accompanied by a large body of theorems [9], [10], [11]. The Archive of Formal Proofs[6] (AFP) has several useful libraries; for example, we used Eberl's library for calculating angles [20]. Combining libraries with the flexible syntax of Isabelle, the program notation of Isabelle/UTP, and our matrix syntax, we can achieve a fairly direct translation of Octave functions, as Figure 5 illustrates. Verification can be automated by the *hoare-auto* tactic, though this depends on arithmetic lemma libraries, some of which we needed to prove manually for the verification. Nevertheless, in our experience, *sledgehammer* [8] performs quite well with arithmetic problems. Moreover, Isabelle has the approximation tactic, which can prove real and transcendental inequalities [21].

For the dynamics, it is necessary to produce an explicit system of first order ODEs, as shown in Definition III.2. Consequently, any algebraic equations must be converted. For example, we could not include the value of $\phi$, but needed to give its derivative and include an axiom linking this with $s$ and $\boldsymbol{v}$. The challenge is finding invariants, and having sufficient background lemmas to prove the verification conditions.

There have been previous works on integrating NC with deductive verification. Notably, Zhan et al. [22] have used Hybrid CSP and an accompanying Hoare logic to verify Simulink block diagrams in Isabelle. Our work is more modest, in that we focus on sequential hybrid programs, but with a transparent translation and a high degree of automation. The dominant and most automated tool for hybrid systems deductive verification remains KeYmaera X [6], [7]. Nevertheless, we believe that our preliminary results show the advantages of targeting Isabelle. Firstly, this allows integration of a variety of mathematical libraries to support reasoning about matrices and transcendental functions, which are both currently unsupported by KeYmaera X. Secondly, we can combine notations with ODEs, and in the future aim to support refinement to code using libraries like Isabelle/C [23]. Thirdly, as illustrated by the obstacle register, with Isabelle/HOL we have the potential to extend $\mathsf{d}\mathcal{L}$ with additional features like collections as used in quantified $\mathsf{d}\mathcal{L}$ [24].

[6]Archive of Formal Proofs. https://www.isa-afp.org/.


## Acknowledgements

We thank Colin O'Halloran and Nick Tudor from D-RisQ for their support with the case study. This research is funded by the CyPhyAssure project[7] (EPSRC grant EP/S001190/1) and the Assuring Autonomy International Programme.


[7]CyPhyAssure Project: https://www.cs.york.ac.uk/circus/CyPhyAssure/

## References


[1] M. Farrell, M. Luckcuck, and M. Fisher, "Robotics and integrated formal methods: Necessity meets opportunity," in *Proc. 14th. Intl. Conf. on Integrated Formal Methods (iFM)*, vol. LNCS 11023. Springer, 2018.

[2] M. Gleirscher, S. Foster, and J. Woodcock, "New opportunities for integrated formal methods," *ACM Comput. Surv.*, vol. 52, no. 6, 2019.

[3] A. Platzer, "Differential dynamic logic for hybrid systems," *J. Autom Reasoning*, vol. 41, pp. 143–189, June 2008.

[4] T. Nipkow, M. Wenzel, and L. C. Paulson, *Isabelle/HOL: A Proof Assistant for Higher-Order Logic*. Springer, 2002, vol. LNCS 2283.

[5] J. H. Y. Munive, G. Struth, and S. Foster, "Differential Hoare logics and refinement calculi for hybrid systems with Isabelle/HOL," in *RAMiCS*, ser. LNCS, vol. 12062. Springer, April 2020.

[6] S. Mitsch, K. Ghorbal, D. Vogelbacher, and A. Platzer, "Formal verification of obstacle avoidance and navigation of ground robots," *International Journal of Robotics Research*, vol. 36, no. 12, 2017.

[7] N. Fulton, S. Mitsch, J.-D. Quesel, M. Völp, and A. Platzer, "KeYmaera X: An axiomatic tactical theorem prover for hybrid systems," in *CADE-25*, ser. LNCS, vol. 9195. Springer, 2015, pp. 527–538.

[8] J. Blanchette, L. Bulwahn, and T. Nipkow, "Automatic proof and disproof in Isabelle/HOL," in *FroCoS*, ser. LNCS, vol. 6989. Springer, 2011.

[9] J. Harrison, "A HOL theory of Euclidean space," in *TPHOLs*, ser. LNCS, J. Hurd and T. Melham, Eds., vol. 3603. Oxford, UK: Springer, 2005.

[10] F. Immler and J. Hölzl, "Numerical analysis of Ordinary Differential Equations in Isabelle/HOL," in *ITP*, vol. LNCS 7406. Springer, 2012.

[11] F. Immler, "Formally verified computation of enclosures of solutions of Ordinary Differential Equations," in *Proc. 6th NASA Formal Methods Symposium (NFM)*, ser. LNCS, vol. 8430. Springer, 2014.

[12] S. Foster, J. Baxter, A. Cavalcanti, J. Woodcock, and F. Zeyda, "Unifying semantic foundations for automated verification tools in Isabelle/UTP," *Science of Computer Programming*, vol. 197, October 2020.

[13] C. A. R. Hoare and J. He, *Unifying Theories of Programming*. Prentice-Hall, 1998.

[14] J. H. Y. Munive and G. Struth, "Verifying hybrid systems with modal Kleene algebra," in *RAMICS*, ser. LNCS, vol. 11194. Springer, 2018.

[15] S. Foster, Y. Nemouchi, C. O'Halloran, N. Tudor, and K. Stephenson, "Formal model-based assurance cases in Isabelle/SACM: An autonomous underwater vehicle case study," in *Proc. 8th Intl. Conf on Formal Methods in Software Engineering (FormaliSE)*. ACM, 2020.

[16] M. Gleirscher, S. Foster, and Y. Nemouchi, "Evolution of formal model-based assurance cases for autonomous robots," in *SEFM*, ser. LNCS 11724. Springer, 2019, pp. 87–104.

[17] R. Calinescu, D. Weyns, S. Gerasimou, M. U. Iftikhar, I. Habli, and T. Kelly, "Engineering trustworthy self-adaptive software with dynamic assurance cases," *IEEE Trans. Softw. Eng.*, vol. 44, no. 11, 2017.

[18] K. Ghorbal and A. Platzer, "Characterizing algebraic invariants by differential radical invariants," in *TACAS*, vol. LNCS 8413. Springer, 2014.

[19] J. Foster, M. Greenwald, J. Moore, B. Pierce, and A. Schmitt, "Combinators for bidirectional tree transformations: A linguistic approach to the view-update problem," *ACM Trans. Program. Lang. Syst.*, vol. 29, no. 3, May 2007.

[20] M. Eberl, "Basic geometric properties of triangles," *Archive of Formal Proofs*, Dec. 2015, http://isa-afp.org/entries/Triangle.html.

[21] J. Hölzl, "Proving inequalities over reals with computation in Isabelle/HOL," in *PLMMS*. ACM, August 2009.

[22] L. Zou, N. Zhan, S. Wang, M. Fränzle, and S. Qin, "Verifying Simulink diagrams via a Hybrid Hoare Logic Prover," in *Proc. Intl. Conf on Embedded Systems (EMSOFT)*. IEEE, 2013.

[23] F. Tuong and B. Wolff, "Deeply integrating C11 code support into Isabelle/PIDE," in *F-IDE*, ser. EPTCS, vol. 310, 2019, pp. 13–28.

[24] A. Platzer, "Quantified differential dynamic logic for distributed hybrid systems," in *CSL*, ser. LNCS, vol. 6247. Springer, 2010, pp. 469–483.